REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-04-2015	Master's Thesis	21-07-2014 to 12-06-2015

4. TITLE AND SUBTITLE Seizing the Digital High Ground: Military Operations and Politics in the Social Media Era	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR Lt Col Andrew Ridland, British Army	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Forces Staff College, Joint Advanced Warfighting School, 7800 Hampton Blvd, Norfolk, VA 23511-1702	**8. PERFORMING ORGANIZATION REPORT**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The information revolution, and in particular the rapid proliferation of social media, is changing how society operates. Confidentiality is being replaced by openness; information that was hitherto the preserve of a few is now instantaneously broadcast around the globe. Cultures, societies, businesses, and disparate individuals are being connected in unprecedented ways, with a profound impact on the traditional balance of power. For those concerned with national security, social media has become one of the most influential factors shaping the operational environment. The British military's current doctrinal view of social media is limited and can perhaps be best characterised as one of caution. Opinion is divided on the relative threats and opportunities. Through the analysis of social media's technological evolution, its impact on crowd behaviour, and using case studies of the Arab Spring and Islamic State, this thesis argues that unless there is a vastly improved understanding of the utility of social media and a greater investment in its application, the military risks losing relevance and becoming a blunt instrument for the execution of political aims and the provision of security in the twenty-first century. Ten specific recommendations are made to help optimise the military for defending the nation's interests in the social media era, including altering the mindset, revising extant doctrine, and selecting and training leaders for the future operating environment.

15. SUBJECT TERMS
Social Media, Information Age, Information Revolution, Islamic State, IS, ISIS, ISIL, Arab Spring, Military Operations, Crowd Behaviour

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	Unclassified Unlimited	49	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified			757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

Seizing the Digital High Ground: Military Operations and Politics in the Social Media Era

Lt Col Andrew Ridland

British Army

This page intentionally left blank

SEIZING THE DIGITAL HIGH GROUND:

MILITARY OPERATIONS AND POLITICS IN THE SOCIAL MEDIA ERA

by

Lt Col Andrew Ridland

British Army

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College, the Department of Defense, or the UK Ministry of Defence.

This paper is entirely my own work except as documented in footnotes.

Signature: _____

13 April 2015

Thesis Adviser: Signature: _____

Dr. Mike Pavelec, PhD
Thesis Advisor

Approved by: Signature: _____

CAPT Steven Guiliani, USN
Committee Member

Signature: _____

Dr. Robert Antis, PhD
Committee Member

This page intentionally left blank

ABSTRACT

The information revolution, and in particular the rapid proliferation of social media, is changing how society operates. Confidentiality is being replaced by openness; information that was hitherto the preserve of a few is now instantaneously broadcast around the globe. Cultures, societies, businesses, and disparate individuals are being connected in unprecedented ways, with a profound impact on the traditional balance of power. For those concerned with national security, social media has become one of the most influential factors shaping the operational environment. The British military's current doctrinal view of social media is limited and can perhaps be best characterised as one of caution. Opinion is divided on the relative threats and opportunities. Through the analysis of social media's technological evolution, its impact on crowd behaviour, and using case studies of the Arab Spring and Islamic State, this thesis argues that unless there is a vastly improved understanding of the utility of social media and a greater investment in its application, the military risks losing relevance and becoming a blunt instrument for the execution of political aims and the provision of security in the twenty-first century. Ten specific recommendations are made to help optimise the military for defending the nation's interests in the social media era, including altering the mindset, revising extant doctrine, and selecting and training leaders for the future operating environment.

ACKNOWLEDGEMENT

I would like to thank Dr. Keith Dixon and Dr. Mike Pavelec from the Joint Forces Staff College for their guidance and advice throughout the research and writing of this thesis.

TABLE OF CONTENTS

This page intentionally left blank

1. INTRODUCTION

In their influential work, *War and Anti-war: Survival at the Dawn of the 21st Century,* Alvin and Heidi Toffler argue that humanity is entering a new, third wave of civilization. In the wake of the agricultural and industrial revolutions, society is now moving into the information age. Both in conflict, and within society at large, knowledge is becoming the central resource. At the heart of their work is the notion that the manner in which society operates— chiefly, how it produces wealth— will generally determine how it wages war.[1] The rapid proliferation of social media is changing the way society operates. Confidentiality is being replaced by openness; information that was hitherto the preserve of a few is now instantaneously broadcast around the globe to an increasingly wide audience. Cultures, societies, businesses and disparate individuals are being connected in unprecedented ways. Social media has helped topple governments, played a key role in democratic elections, been used to recruit terrorists, and inspired mass movements. The changes to the availability and dissemination of information by social media is having a profound impact on the traditional balance of power. For those concerned with national security, social media has become one of the most influential factors shaping the operational environment.

Whilst the precise manner in which social media will evolve over the coming years is unclear, its growth, its significance, and its influence on national security is without doubt. U.S. President Barack Obama believes that, "technology is empowering civil society in ways no iron fist can control."[2] Robert Hannigan, Director of Britain's

[1] Alvin Toffler and Heidi Toffler, *War And Anti-War* (Boston: Little, Brown, 1993).
[2] Barack Obama, "Remarks By The President At The United States Military Academy Commencement Ceremony", *The White House*, last modified 2014, accessed November 17, 2014,

Government Communications Headquarters (GCHQ), has stated that social media has become the command and control network of choice for terrorists and criminals.[3] In November 2012, Israel became the first nation to initiate hostilities by social media, launching Operation Pillar of Defence with a YouTube video of the assassination of Hamas leader Ahmed al-Jabari. Facebook's CEO, Mark Zuckerberg, believes that, "society has reached another tipping point ... by giving people the power to share, we are starting to see people make their voices heard on a different scale from what has historically been possible. These voices will increase in number and volume. They cannot be ignored. Over time, we expect governments will become more responsive to issues and concerns raised directly by all their people rather than through intermediaries controlled by a select few."[4] If, as David Lonsdale postulates, information becomes the dominant factor in warfare, with information dominance as the defining war-winning characteristic, the ability to master and manipulate social media is now fundamental to the provision of effective security for the nation.[5]

The British military's current doctrinal view of social media is limited and can perhaps be best characterised as one of caution. Opinion is divided on the relative threats and opportunities. In its recently published *Cyber Primer*, the UK Ministry of Defence (MOD) makes few explicit references to social media, but does so in the context of the threats that it poses to the operational security of individuals and to the broader political

---

http://www.whitehouse.gov/the-press-office/2014/05/28/remarks-president-united-states-military-academy-commencement-ceremony.

[3] Robert Hannigan, "The Web Is A Terrorist's Command and Control Network Of Choice - FT.Com", *Financial Times*, last modified 2014, accessed January 4, 2015, http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3LFmC9nwL.

[4] BBC News, "Zuckerberg's Letter To Investors", last modified 2012, accessed December 10, 2014, http://www.bbc.com/news/technology-16859527.

[5] David J Lonsdale, *The Nature Of War In The Information Age* (London: Frank Cass, 2004).

and commercial manipulation that can occur. Extant Media Operations and Information Operations Joint Doctrine Publications do not mention it all.

Through the analysis of social media's technological evolution, its impact on crowd behaviour, and using case studies of the Arab Spring and Islamic State, this thesis will argue that unless there is a vastly improved understanding of the utility of social media and a greater investment in its application, the military risks losing relevance and becoming a blunt instrument for the execution of political aims and the provision of security in the twenty-first century.

2. WHAT IS SOCIAL MEDIA AND WHY DOES IT MATTER?

Just as the ecology of social media is constantly changing so, it appears, are commonly accepted definitions of the term. Indeed, despite the ever-increasing number of people using social media, and also the literature about it, there still seems to be a very limited common understanding of exactly what the term means. For the purposes of this thesis, social media has been defined as *websites and applications that enable users to create, share, and modify content, or to participate in social networking.*[6]

The Origins of Social Media

The first commonly recognizable social networking site appeared in 1997 when SixDegrees allowed users to create profiles, list their friends, and add friends-of-friends to their own lists.[7] SixDegrees promoted itself as a tool to help people connect and send messages to others; however, despite attracting millions of users, it collapsed in 2000 after failing to maintain a sustainable business model. Despite its relatively short life-span, this pioneering social networking site had done something unique. It had not simply allowed individuals to meet strangers, it had enabled users to articulate and make visible their social network, which in turn created latent or weak ties between individuals who would not otherwise have made an offline connection.[8]

---

[6] A deliberately broad definition has been used as the more specific distinctions that can be drawn between related concepts such as Web 2.0, User Generated Content, social networking sites, and blogs are not considered relevant for the arguments and recommendations proposed. Web 2.0 is a term used to describe the way in which software developers and end-users utilize the World Wide Web as a platform whereby content and applications are no longer created and published by individuals, but instead are constantly modified by all users in a participatory and collaborative fashion. User Generated Content can be seen as the sum of all ways in which people use social media. See Andreas M. Kaplan and Michael Haenlein, "Users Of The World, Unite! The Challenges And Opportunities Of Social Media", *Business Horizons* 53, no. 1 (2010): 59-68.

[7] Danah M. Boyd and Nicole B. Ellison, "Social Network Sites: Definition, History, And Scholarship", *Journal of Computer-Mediated Communication* 13, no. 1 (2007): 210-230.

[8] Caroline Haythornthwaite, "Social Networks And Internet Connectivity Effects", *Information, Communication & Society* 8, no. 2 (2005), 125-147.

In the months and years following the appearance of SixDegrees, there was an explosion of networking sites and community tools supporting various combinations of profiles and publicly shared contacts. AsianAvenue, BlackPlanet, and MiGente allowed users to create personal, professional, and dating profiles, Ryze helped people leverage their business networks, but it was arguably Friendster, MySpace, and Facebook that really shaped the business, cultural, and research landscape.[9]

The Social Media Landscape Today

A rich, interconnected, and diverse ecosystem of social media sites now exists varying widely in functionality and content. Some, such as Facebook, are for individuals; while others, such as LinkedIn, are more focused on professional networks. Media sharing sites, such as MySpace, YouTube, Instagram, and Flickr concentrate on shared videos and photos. Blogs have become an important source of public opinion that have dramatically altered the traditional corporate media environment and the recent phenomenon of micro-blogging, represented by Twitter, perhaps the best-known micro-blogging site, has exploded since its inception in 2006. Twitter was, at one stage, signing up 370,000 new users every 24 hours, and currently has more than 145 million users sending an average of 90 million 'tweets' a day.[10] It is now seen by many as an indispensible part of individual, as well as public and corporate, diurnal activity. Significantly, most websites now have direct links to the most popular social media sites,

[9] Boyd and Ellison, Social Network Sites: Definition, History, And Scholarship, 212.
[10] Gabriel Madway, "Twitter Remakes Website, Adds New Features", *Reuters*, last modified 2014, accessed January 3, 2015, http://www.reuters.com/article/2010/09/15/us-twitter-website-idUSTRE68E02620100915.

thus providing an even greater degree of connectivity and influence. A visual representation of the global social media landscape in 2014 is shown in Figure 1.

Figure 1. Social Media Landscape 2014 – A Global Social Web[11]

According to The Global Web Index's Q2 2014 report, Facebook is the number one global social network – and by quite some margin.[12] Excluding China, 82 per cent of Internet users aged 16-64 now have a Facebook account. Its overall reach continues to increase. Three platforms compete for second position behind Facebook: Google+, YouTube, and Twitter. Google+ has been performing especially well in emerging Internet markets and has seen a 10 per cent increase in account members over the last year. YouTube tends to take second place in mature Internet markets, whilst Twitter, which overtakes Facebook to claim first place in Japan, has seen a 7 per cent increase in

[11] Frédéric Cavazza, "Social Media Landscape 2014 - Fredcavazza.Net", *Fredcavazza.Net*, last modified 2014, accessed January 3, 2015, http://www.fredcavazza.net/2014/05/22/social-media-landscape-2014/.
[12] Insight.globalwebindex.net, "GWI Social - Q2 2014 | Globalwebindex Report Series", last modified 2014, accessed December 9, 2014, http://insight.globalwebindex.net/gwi-social-q2-2014.

members in the last twelve months.[13] What these statistics show, is that if Facebook were a state, its population would rival that of the most populous country on Earth. According to the site's 2014 Q3 Earnings Report, the number of monthly active users is now over 1.35 billion – roughly equivalent to the population of China and 9 per cent larger than that of India.[14] Nearly a fifth of the world's population logs onto Facebook once a month. Figure 2 shows how Facebook's population compares with various others around the world.

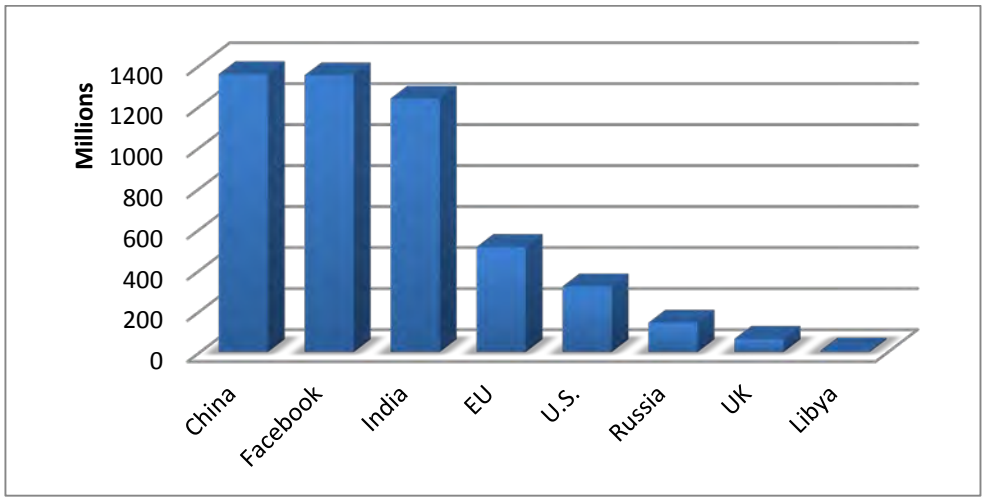

Figure 2. Facebook's Population Size as a Comparison[15]

Whilst these figures provide an interesting numerical comparison, they also underscore the breadth of information a company like Facebook has about the online lives and identities of its population when compared to a state, as well as the potential influence this provides. Figure 3 shows the current user community sizes of the most popular social media sites.

---

[13] Insight.globalwebindex.net, "GWI Social - Q2 2014 | Globalwebindex Report Series", last modified 2015, accessed January 4, 2015, http://insight.globalwebindex.net/gwi-social-q2-2014.
[14] Investor.fb.com, "Facebook Reports Third Quarter 2014 Results – Facebook", last modified 2014, accessed January 5, 2015, http://investor.fb.com/releasedetail.cfm?ReleaseID=878726.
[15] Source: created by the author using data from The CIA World Factbook available at: https://www.cia.gov/library/publications/the-world-factbook/rankorder/2119rank.html

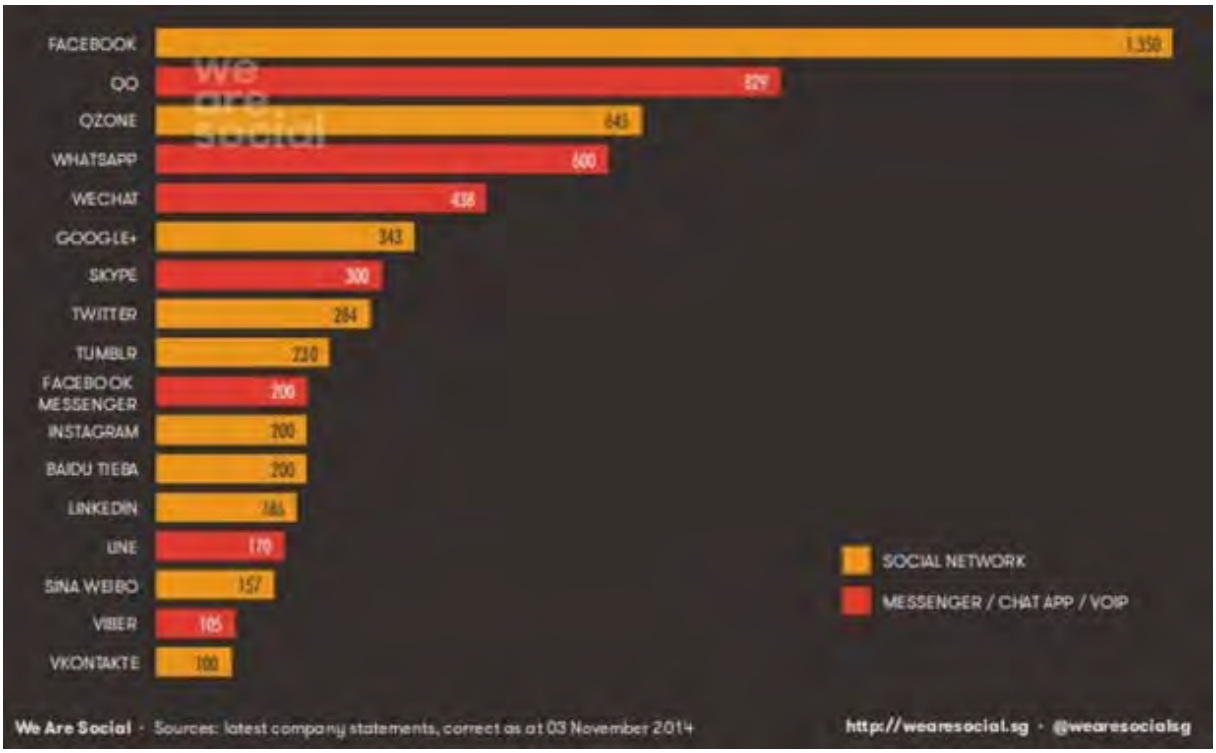

Figure 3. Comparison of Social Media User Numbers (in millions)[16]

Implications for Society

The implications of the global proliferation of social media and the increasing interpenetration within society are significant and extensive. Whereas at the outset, due to the requirement of computer technology and transmission bandwidth, social media sites spread primarily in the developed world, the shift towards mobile technology has made much broader global propagation possible. For the duration that Moore's Law, with its resultant implications for computer size, cost, and processing power, continues to be valid, this spread is only going to increase.[17] Indeed, capitalised market forces make it

[16] We Are Social, 'Blog', last modified 2014, accessed January 4, 2015, http://wearesocial.com.
[17] Moore's Law is a computing term that originated around 1970 and for many years provided the basic business model for the semiconductor industry. The simplified version of this law states that processor speeds, or overall processing power for computers, will double every two years – and the corollary that the price of computers (and thus smart phones) will drop precipitately, see R.R. Schaller, 'Moore's Law: Past, Present And Future', *IEEE Spectr.* 34, no. 6 (1997), 52-59.

unstoppable. A current snapshot of global Internet and mobile phone usage is shown in Figure 4, whilst Figure 5 gives as indication of Internet penetration by region.

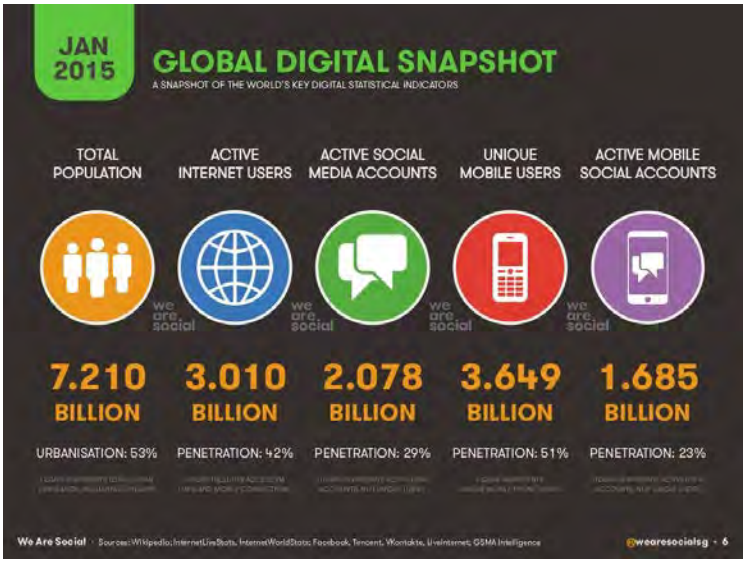

Figure 4. Global Digital Snapshot

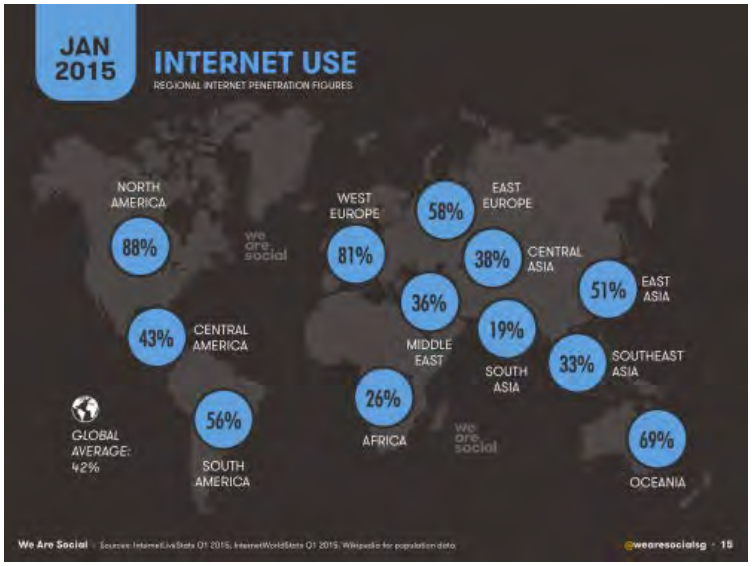

Figure 5. Internet Penetration by Region [18]

Analysis of historical global mobile phone ownership helps provide a degree of scale for the recent growth. According to a Pew survey, in 2007, 81 per cent of

[18] We Are Social, 'Blog', last modified 2015, accessed February 24, 2015, http://wearesocial.com.

Americans owned a mobile phone, a 20 per cent increase compared with 2002. The median increase in ownership for all countries surveyed over the same period was 24 per cent. The most rapid growth was in Russia, which went from 8 per cent to 65 per cent over the five-year period. Looking at mobile phone usage over the same timeframe, of the countries surveyed, Nigeria recorded the fastest expansion with 67 per cent, whilst Indonesia ranked last, but still with 24 per cent.[19]

Hitherto, the majority of social media sites have developed relatively unimpeded by national legislation, mainly because they originate in countries with constitutional rights for freedom of speech. But, with mobile technology in developing countries increasingly becoming the standard communication method, social media is now taking root in less developed, often non-democratic, authoritarian countries. The potential for changing the relationship between the people and their government has enormous operational and strategic significance.

Despite, or perhaps because of, its increasingly ubiquitous nature, the very use of social media as an instrument for information transfer can be detrimental to a state's security. It can be argued that the higher the degree to which a society is dependent on the use of information technology, with its correspondingly high ratio of online information acquisition, sharing, and control, the higher its vulnerability to web-based threats.[20] Accordingly, the risks of incorporating social media applications in the day-to-day running of a country, either in strategically important companies, national infrastructure,

[19] James Jay Carafano, *Wiki At War* (College Station: Texas A&M University Press, 2012), 89.
[20] Gustav Lindström, "Meeting the Cyber Security Challenge," Geneva Centre for Security Policy, Geneva Paper 2012/7 (June 2012); available at http://www.gcsp.ch/Regional-Capacity-Development/Publications/GCSP-Publications/Geneva-Papers/Research-Series/Meeting-the- Cyber-Security-Challenge.

or in government agencies, might appear higher for more developed nations. It is a point reinforced by Richard Clarke, the former White House National Coordinator for Security, Infrastructure Protection, and Counterterrorism, who argues that despite having less advanced offensive cyber capabilities, China, Russia, North Korea, and Iran all rank above the U.S. in overall cyber war strength.[21] The principal reason being the disparity between their respective defensive cyber capabilities when set alongside their relative online dependence. China, for example, scores highly with respect to cyber defence, in part because it has plans and the capability to disconnect the entire nation's network from the rest of cyberspace. America, by contrast, currently has neither the plans nor capability, because the majority of cyber connections into America are owned and operated by private corporations. North Korea scores highly because of relatively good cyber defence capabilities as well as very low dependence, given that it has limited critical infrastructures reliant on networked systems.[22]

In addition to these more obvious security issues, there are other implications caused by the proliferation of social media, two of which are of particular significance. The first is that secrets are now increasingly difficult to keep. Smartphone technology allows numerous possibilities for users to interact, transfer, and obtain digital information. Mobile phone cameras can be found almost everywhere and it will not be long before one will be able to say that wherever there are people, there will be cameras with the ability to instantaneously share events with a global audience. Content uploaded onto the website LiveLeak.com, for example, illustrates the potential for any isolated event to become an international sensation.

[21] Richard A Clarke and Robert K Knake, *Cyber War* (New York: Ecco, 2010), 148
[22] Ibid.

The second is that social media provides a platform for civil society to influence the public sphere.[23] Society now has the ability to access information, share ideas, and express support for, or reject, government policies at anytime and from anywhere. In democracies, this is not necessarily a significant factor; in semi-authoritarian states, it can be a threat to regime survival. The increasing use of social media can create a rapid public response to political decisions or actions. It is possible that during a crisis, the public will be reacting to information obtained through social media long before the government can gather data and provide its assessment, or its version of events. Furthermore, in order to win public support, the need for transparent decision-making is increasing. Due to this continuous supervision of politics, the reaction time for governments (compared to the pre-social media era) has been dramatically reduced. A possible by-product of this in democracies might be for politicians to become increasingly risk averse and cautious when making decisions, given that mistakes will be quickly exposed to the public. [24] Yet in times of crisis, this is not always necessarily the best approach to national strategic leadership.

That said, governments can clearly use social media to their advantage. If utilised and exploited properly by government agencies, they can unlock self-organizing capabilities within government, promote networking and collaboration with groups outside government, speed up decision-making, and increase agility and adaptability. Security organisations can decrease the probability of being surprised, or even

[23] Where civil society is understood as the organized expression of the values and interests of society. From M. Castells, 'The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance', *The Annals of the American Academy of Political and Social Science* 616, no.1(2008): 78-93.
[24] Marko Papic and Sean Noonan, "Social Media as a Tool for Protest," *Security Weekly* (3 February 2011); available at http://www.stratfor.com/weekly/20110202-social-media-tool- protest.

outmanoeuvred.[25] Seen in this light, social media could act in a positive way as a warning and prevention tool or, if used appropriately, as a manipulation device to prevent violence.[26]

Of course, this advantage is equally available to open as well as repressive regimes. As social media becomes more ubiquitous, both people and governments will continue to discover and employ new dimensions to this global phenomenon that will undoubtedly shape the course of the twenty-first century.

[25] Mark Drapeau and Linton Wells II, "Social Software and National Security: An Initial Net Assessment," Center for Technology and National Security Policy Defense & Technology Paper, National Defense University, Washington, D.C. (April 2009), 1; available at www.dtic.mil/ cgi-bin/GetTRDoc?AD=ADA497525.
[26] Thorsten Hochwald, "How Do Social Media Affect Intra-State Conflicts Other Than War?", *ConnQJ* 12, no. 3 (2013): 9-37.

3. THE MILITARY'S CURRENT VIEW OF SOCIAL MEDIA

Information has always been important in warfare, however it is only in the latter part of the twentieth century that it emerged as the nucleus of a new "central mode of warfare," which put activities related to the production, dissemination, and utilization of information to support communication and decision-making at its very heart.[27] A concept that flows from this, and one that is fundamental to British doctrine and taught widely at various levels of training, is the notion that decision-making occurs in recurring cycles of observe-orient-decide-act: the OODA loop. The idea was developed by USAF pilot and military strategist John Boyd and it explains how a competitive advantage can be achieved when dealing with human opponents by favouring agility over raw power. It is applicable whether one is fighting in a trench, in the middle of an aerial dogfight, or even in the art of Generalship. In sum, he who acts correctly first wins; the decisive advantage going to the opponent who can operate 'inside' the other's OODA loop, and make decisions faster than the enemy's ability to do so.

The heavy reliance on computer-based information systems in military organisations and the information these systems store and transmit has become an operational construct unto itself. Given the importance of information and influence, information-related activities in the military environment have their own specific term. Officially referred to as Information Operations (Info Ops), British doctrine provides the following definition:

> "coordinated actions undertaken to influence an adversary or potential adversary in support of political and military objectives by undermining his will, cohesion and decision-making ability, through affecting his information, information based

[27] Tami Davis Biddle, *Rhetoric And Reality In Air Warfare* (Princeton, N.J.: Princeton University Press, 2002).

> processes and systems, while protecting ones own decision-makers and decision-making processes."[28]

There is a clear connection to the ability to make decisions and the means to transmit or receive information. It is believed that by influencing this relationship in some way, the adversary's will to fight and his capability to fight will be affected.

Info Ops are employed with the intent of "influencing will and … affecting those capabilities that directly enable the application of will."[29] A wide variety of tools are used to orchestrate and synchronize a range of activities to achieve this intent. Doctrine lists them as: "psychological operations; presence, posture, and profile; operational security; deception; electronic warfare; physical destruction; and computer network operations."[30] Whilst suitably broad ranging and reasonably comprehensive, the extant doctrine lists only military-related capabilities, often completely separate from the inter-connected global social network. Not once is social media specifically mentioned.

If Info Ops seek to affect the application of will, what also appears to be lacking in extant doctrine is the interpretation of information as image or perception; where information can be used "as a resource for the shaping of perception and imaginary," or as a vital tool to shape a "particular image about a given situation or thing."[31] Walid Phares explores this concept in what he categorises as the West's war of democracy against terrorism, arguing that the most important battle is the one currently taking place in the hearts and minds of the world's population.[32] It is a view that has important

---

[28] UK Ministry of Defence, *Information Operations*, Joint Warfare Publication 3-80 (London: MOD, June 2002).
[29] Ibid
[30] Ibid.
[31]Elgin M Brunner and Myriam Dunn Cavelty, "The Formation Of Information By The US Military: Articulation And Enactment Of Infomanic Threat Imaginaries On The Immaterial Battlefield Of Perception", *Cambridge Review of International Affairs* 22, no. 4 (2009): 629-646.
[32] Walid Phares, *The War Of Ideas* (New York: Palgrave Macmillan, 2007).

parallels to similar concepts such as 'fourth generation warfare,' 'asymmetric warfare,' 'softwar,' and 'netwar' amongst others.[33] In the information age, these concepts emphasize the growing importance of the non-physical, political and narrative aspects of warfare, frequently citing the 'war on terror' as providing clear evidence that a substantial shift in the nature of global conflict has occurred.

The arguably narrow view taken by the UK on Info Ops can be further contrasted with that of current Russian thinking. Whereas Info Ops from the British military perspective predominantly focuses on physical infrastructure and military command and control, Russia, because of its historical experience and the legacy of Soviet thinking, sees Info Ops in a subtly different light. Whilst not disparaging their usefulness for these purposes, Russian thinkers see Info Ops as a new means to conduct large-scale political warfare to reshape the thinking of an entire political community.[34] They believe that a state's domestic structures have become the object of governments' discourse about security and, particularly with regard to Info Ops, a potential target of adversaries.[35] In other words, by manipulating the information environment of an adversary's domestic society, one can influence their government's decision making to suit one's own needs. General Valery Gerasimov, Chief of the General Staff of the Russian Federation, elaborates on this role of Info Ops in warfare:

> "The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness … All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces - often under the guise of

[33] Sean Lawson, "The US Military's Social Media Civil War: Technology As Antagonism In Discourses Of Information-Age Conflict", *Cambridge Review of International Affairs* 27, no. 2 (2013): 226-245.
[34] Stephen Blank, "Russian Information Warfare As Domestic Counterinsurgency", *American Foreign Policy Interests* 35, no. 1 (2013): 31-44.
[35] Ibid.

> peacekeeping and crisis regulation - is resorted to only at a certain stage, primarily for the achievement of final success in the conflict…The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy. In North Africa, we witnessed the use of technologies for influencing state structures and the population with the help of information networks."[36]

Gerasimov could have added other examples closer to home: that of Georgia in 2007 and Ukraine in 2014. While the Russians have a strong appreciation for non-official information networks that is lacking in British Info Ops doctrine, even in the extant Media Operations Joint Doctrine Publication, there is no mention of social media. The following excerpt provides an overview of the British military doctrinal approach:

> "The aim of Media Operations (Media Ops) is to promote widespread understanding and support for military operations while maintaining Operational Security (OPSEC). The primary purpose of Media Ops is to communicate information to audiences, through the medium of national and international media. Their main effort in any military operation is to communicate the principal themes and messages in pursuit of the end-state, whilst remaining sensitive to media interests. They are an integral part of any military operation. Although Media Ops is primarily focused on the need to maintain domestic public support and hence freedom of action, its impact is much wider. Media Ops will also have an influence on adversaries, allies and uncommitted parties. It is therefore essential that Media Ops staff and Info Ops staff work closely together to ensure that the desired message is put across to the intended audiences … To avoid giving the false impression that the media are being manipulated in any way, a distinction must be maintained between Info Ops and Media Ops."[37]

Like Info Ops doctrine, Media Ops is focused on supporting military operations. Although the doctrine stresses the use of national and international information systems, its intent is to create positive reactions amongst the target audience(s) through content. It is not focused on the medium, which in the globalized world, truly is the message. In contrast to Russian views, British doctrine sees a distinct separation between Info Ops

---

[36] Mark Galeotti, 'The 'Gerasimov Doctrine' And Russian Non-Linear War', *In Moscow's Shadows*, last modified 2014, accessed October 29, 2014, http://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[37] UK Ministry of Defence, *Media Operations*, Joint Doctrine Publication 3-45.1(London: MOD, September 2007).

and Media Ops. The reality is that social media—the medium itself, as Marshall McLuhan famously observed—is now more powerful than the message content being carried by the medium.[38] The concentration on process as opposed to function is a weakness in British doctrine, reflecting a seriously outdated concept of how information is used and travels in the twenty-first century.

The MOD's unclassified *Cyber Primer*, published in December 2013, provides a baseline awareness of the cyber domain for the UK Defence audience and articulates the importance of the cyber domain across all military disciplines. It does make reference to social media, but does so in the context of the threat that it poses, both to the operational security of individuals, and the wider political and commercial manipulation that can occur.[39] Joint Doctrine Note 3/13 also advises commanders to, "exploit cyber capabilities as part of information activities directed at different audiences," and makes reference to digital networks and how words, images, and actions in cyberspace can affect perceptions of legitimacy and thus campaign success.[40] The centrality of influence and the importance of the battle for the narrative in ensuring the success of military operations are also emphasized in *The Future Character of Conflict*, a doctrinal publication written ahead of the UK 2010 Strategic Defence and Security Review.[41]

Although these various publications and a number of other doctrine notes individually mention aspects of cyber operations, acknowledge various digital networks, and/or recognise the importance of influence, the thread that pulls them together and knits

[38] Marshall McLuhan and Quentin Fiore, *The Medium is the Massage* (New York: Random House, 1967)
[39] Gov.uk, 'Cyber Primer - Publications - GOV.UK', last modified 2014, accessed October 22, 2014, https://www.gov.uk/government/publications/cyber-primer.
[40] UK Ministry of Defence. *Cyber Operations – The Defence Contribution*, Joint Doctrine Note (JDN) 3/13. London: MOD, August 2013.
[41] UK Ministry of Defence, *Future Character Of Conflict*, (London: MOD, 2010)

greater global connectivity, social media, crowd behaviour and Info Ops is currently lacking. The link between social media's impact on societal perception and behaviour and the recognition that armed conflict is a clash of interests between, or among organized groups, each imposing their will on the opponent, is not sufficiently extrapolated, emphasized or exploited.[42] Furthermore, there is a lack of understanding of the significance social media has on societal perception and behaviour within the context of military operations across the continuum of conflict.

[42] Definition of armed conflict taken from United States Army, *Strategic Landpower*, (TRADOC, 2104).

4. HOW THE FEW CAN INFLUENCE THE MANY

In his seminal book, *Here Comes Everybody*, about the effect of the Internet on modern group dynamics and organisation, Clay Shirky discusses a graph that explains why Boyd's OODA loop concept has the potential to be so powerful in a socially networked operational environment.[43] He uses an insight derived from Power Law, a special mathematical relationship between two kinds of entities: the frequency of an event and its magnitude. It has been called the Power Law Curve and is shown in Figure 6. It depicts what happens when the frequency of an event decreases at a faster rate than the magnitude of the event increases. A familiar expression that explains this relationship is, "10 per cent of the people do 90 per cent of the work." In a Power Law Distribution Curve, a few entities dominate.[44]

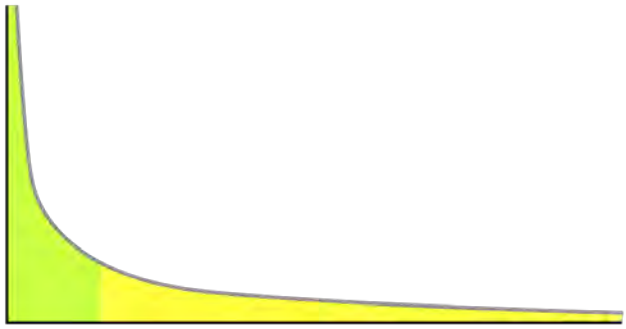

Figure 6. An example of a Power Law Distribution Curve. To the right (yellow) is the long tail; to the left (green) are the few that dominate. In this example, the areas of both regions are equal.[45]

Shirky argues that the Power Law Distribution Curve (rather than a common 'bell curve' that represents what might be termed a normal distribution of data) best describes online behaviour in social networks. At the left end of the curve, a small number of

[43] Clay Shirky, *Here Comes Everybody* (New York: Penguin Press, 2008).
[44] Carafano 2012, 8.
[45] Wikipedia, 'Long Tail', last modified 2015, accessed January 4, 2014, http://en.wikipedia.org/wiki/Long_tail#mediaviewer/File:Long_tail.svg.

participants (from total members in the network) account for most of the activity such as posting and commenting on information. He cites the example of Wikipedia, the online encyclopaedia, which is open to anyone in the world to contribute to or edit. In 2009, the site attracted tens of millions of visitors (individuals that make up the population) but only about 85,000 were active contributors— a small fraction of the network. Within that group, there was a further elite within the elite. For example, "the Wikipedia article for asphalt had 129 contributors making 205 total edits, but the bulk of the work was undertaken by a small fraction of participants, and just six accounted for about a quarter of the edits."[46] To give a sense of scale, in 2009 approximately 65 million people visited at least one Wikipedia page every month. In sum, with big groups online, only a tiny proportion of the population are calling the shots. Therefore, those who occupy the left end of the spectrum in Shirky's Curve are in a powerful position— they are influencing, educating, or directing the rest of the network. The power of the few to influence the many is the reality of social media. The significance of this fact should not be lost on strategists or military planners.

But it is not just within the left end of Shirky's curve that one can find significant factors with the potential to shape military efficacy. On the right hand side, within the yellow tail of the curve, groups are much smaller, so it is correspondingly easier to pass information or have a meaningful exchange of ideas. Here is the place for a tight cluster of conversation where participants contribute in a more equal manner, and the value of each individual contribution is potentially more significant and more influential. If this cluster contains the right blend of people, then knowledge, expertise, and authority can be

[46] Shirky, *Here Comes Everybody*, 123.

combined to pass information and make high-quality decisions quickly— and thus create a faster OODA loop.[47]

As any soldier will appreciate, the occupation of high ground on the battlefield has provided a military advantage to armies for centuries. Seizing the high ground is still a fundamental concept to success in the modern combined arms battle space. The deductions drawn from Shirky's analysis of social networking demonstrate a new high ground in the terrain of electrons. In the contemporary, interconnected environment where wars are rarely conclusive and, to quote Feargal Cochrane, "the power of war is determined by the fluid relations between a complex network of individuals and groups," the far left and far right of the social networking curve can be categorised as the new high ground.[48] On the far left, in broadcast mode, social networks can be instruments of mass mobilisation. On the far right, in conversation mode, they can be used by virtual teams to move faster and 'get inside' an adversary's OODA loop. Winning the information war at one, or both, of these coordinates on the curve, could well be the difference between success and failure on the battlefield, or in a matter of national security.[49]

The concept of social media's ability to make a substantial impact in the area of decision-making can be taken one step further. One of the fundamental characteristics of the twenty-first century strategic environment is complexity. The sort of operations that the British military are likely to find themselves executing over the course of the next decade will be fluid, and will involve a complex array of direct and indirect actors— state, sub-state, and frequently transnational. For the operational planner or strategist, the

[47] Carafano, *Wiki At War*, 10.
[48] Feargal Cochrane, *Ending Wars* (Cambridge: Polity, 2008), 30.
[49] Carafano, *Wiki At War*, 10.

first task is to understand and define the problem. Frequently in the past, analysing the nature of the problem was comparatively simple because adversaries were often well defined and thus provided a relatively sharp degree of focus. However, conflict over the course of the last decade or so has been shown to take many forms with an environmental picture that is increasingly blurred. Aggregating expertise, combining input from different perspectives, and cross-referencing against different sources will significantly enhance the ability of military planners to understand the environment and successfully define the problem.

In his book, *Wisdom of Crowds*, James Surowiecki explores the aggregation of information within groups, which he argues results in decisions that are often better than those that could have been made by any single member of the group. Presenting numerous case studies, he concludes that, "under the right circumstances, groups are remarkably intelligent, and are often smarter than the smartest people in them. Groups do not need to be dominated by exceptionally intelligent people in order to be smart."[50] Some will argue that there are plenty of examples where collective opinion is not wise, or that factors such as bias can have undue influence on an outcome. However, the interconnectivity that social media provides enables commanders, strategists, or planners, to very easily reach out to a large group and create the conditions for better problem solving analysis, or for smarter production of an operational design. The concept extends to the sharing of peer-to-peer experiences, lessons identified from operations, discussions over the latest tactics, techniques, and procedures, and more general professional education. To give a tactical example, across the British Army, having these networks at

[50] James Surowiecki, *The Wisdom Of Crowds* (New York: Doubleday, 2004).

the Platoon, Company, Battalion, and Brigade levels of command could significantly enhance professional competence and combat effectiveness.

5. REVOLUTIONS, REVELATIONS AND REVULSION

The Arab Spring – A Case Study in the Role of Social Media

The use of social media has had a significant impact on the direction of a number of popular movements that have resulted in political change. Indeed, social media has been ranked as the most important factor in the recent transformations of authoritarian regimes in the Middle East and North Africa.[51] These actions, collectively, if hopefully, have been described as the Arab Spring. They have magnified the inherent tension between people desiring access to information and a regime's requirement to deny or control it. This tension lies at the heart of the twenty-first century's political landscape. Author Ivan Sigal has observed that:

> "The discord between citizens creating and disseminating media and governments aspiring to restrict, censor, and influence in conflict situations reflects the tension between informal, fast-moving information and community networks and the formal hierarchies of state power. New information networks link people together through non-state, citizen-oriented communities, challenging the concept of a ruling authority able to control and direct information flows amongst its citizens."[52]

The popular uprisings that have occurred in the region can certainly be traced to the standard sources: weak governance, low economic opportunity, corruption, income inequality, human rights violations, and poor prospects for a burgeoning youth population. However, what has changed to become a major factor is how social media has spread this information and solidified key opposition groups. As frustrations grew, all that was needed was a triggering event. Once such an event occurred, the population

[51] Wael Ghonim, *Revolution 2.0* (Boston: Houghton Mifflin Harcourt, 2012).
[52] Ivan Sigal, "Digital Media in Conflict-Prone Societies," paper prepared for the Center for International Media Assistance (October 2009), 21; available at http://cima.ned.org/sites/ default/files/Sigal%20-%20Digital%20Media%20in%20Conflit-Prone%20Societies.pdf. accessed 8 January 2015.

could mobilize via social media. The following examples will illustrate how social media can rapidly shape and re-shape the strategic and operational environment.

Tunisia

On 17 December 2010, a twenty-six year old Tunisian street vendor named Mohammed Bouazizi committed suicide by self-immolation as a form of protest against price inflation and political repression. Video footage from mobile phones showing the suicide, as well as clashes between protestors and security forces, allowed a dramatic, if isolated event to become national and then international news. Facebook and Twitter played significant roles in disseminating information and mobilising groups. Inevitably, both virtual and real revolutionaries surfaced, protests grew in size and then spread to areas outside the capital city. Less than fifteen days after the street vendor's suicide, Tunisia was in the midst of a popular revolution—what became known as the Jasmine Revolution. President Zine el-Abidine Ben Ali fled into exile, ending a twenty-three year regime, and thus enabling, within a year, democratic elections to take place.

After analyzing this episode, Khaled Koubaa, the President of the Internet Society in Tunisia, reported that of the 2000 registered Twitter users, only 200 were active users, but there were two million users of Facebook. He claims "social media was absolutely crucial … three months before Mohammed Bouazizi burned himself in Sidi Bouzid, we had a similar case in Monastir. But no one knew about it because it was not filmed. What made a difference this time is that the images of Bouazizi were put on Facebook and everyone saw it."[53] Further stressing the role of social media, Habibul Khondker notes

[53] Peter Beaumont, 'The Truth About Twitter, Facebook And The Uprisings In The Arab World', *The Guardian*, last modified 2011, accessed January 28, 2015, http://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings-arab-libya.

that in Tunisia protest movements were crushed in 2008 without a significant backlash. Part of the reason was there were only 28,000 Facebook users at that time, therefore social media penetration was low.[54] By 2010 this number had risen significantly.

In Tunisia, social media was used by protestors as a platform to fill the leadership vacuum; crowds self-organised to generate and sustain momentum in support of their cause. While significant underlying factors created the necessary environmental conditions, Tunisia's rapid progression from civil unrest to violence to revolution, clearly demonstrate the strategic effect that social media can have. Its influence on a crowd, particularly the ability to overcome the obstacles of time and space by orchestrating multiple, simultaneous, and sequential social movements has clear implications for military operations. As will be further explored below, the ramifications of these events were not limited to Tunisia, but had regional and global consequences.

Egypt

In Egypt the majority of the population has access to a mobile phone. After Iran, the country also boasts the region's second largest Internet-using population.[55] News from Tunisia, therefore, spread rapidly, despite limited and begrudging coverage by state-run media. It sparked rumblings of Egyptian discontent. Like Tunisia, Egypt's authoritarian regime had maintained control by banning political parties and limiting media. Social, economic, and political conditions over the preceding decade had, however, created a large cadre of disaffected citizens. Despite their best efforts, the state could not silence them all. When, for example, the Muslim Brotherhood's online news

[54] Habibul Haque Khondker, 'Role Of The New Media In The Arab Spring', *Globalizations* 8, no. 5 (2011): 675-679.
[55] Philip N. Howard and Muzammil M. Hussain, 'The Role Of Digital Media', *Journal of Democracy* 22, no. 3 (2011): 35-48.

service was banned, servers popped up in London and the organization maintained its access to the Egyptian people. However, the triggering event, and what turned anti-Mubarak vitriol into civil disorder, was not an established anarchist group, but a Facebook campaign. Google executive, and accidental activist, Wael Ghonim, started the Facebook group "We are All Khaled Said" to keep alive the memory of a 28-year old blogger who was beaten to death by Egyptian police on 6 June 2010 for exposing internal corruption. It was a moniker to be imitated five years later by the "Je Suis Charlie" solidarity campaign that occurred after the Charlie Hebdo killings in Paris on 7 January 2015. Just as images of Bouazizi's immolation had spread rapidly throughout Tunisia and beyond, so the bloodied and disfigured face of Khaled Said spread from a single mobile phone to thousands in an instant. Two minutes after the page was started, 300 people had joined it. Three months later, that number had grown to more than 250,000.[56] Ghonim also quickly emerged as Egypt's leading voice on Twitter, linking a vast Arab-speaking social network with English-speaking observers overseas.[57]

Figure 7. An Egyptian and a Global Social Network

[56] Jose Vargas, 'How An Egyptian Revolution Began On Facebook', *Nytimes.Com*, last modified 2012, accessed November 19, 2014, http://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html?pagewanted=all&_r=1&.
[57] Philip Howard and Muzammil Hussain, "The Role of Digital Media", *Journal of Democracy* 22, no. 3 (July 2011 2011): 35-48.

What bubbled up online spilled onto the streets, starting with a series of minor protests and culminating in a massive rally at Tahrir Square in Cairo. An increasingly desperate President Hosni Mubarak tried to unplug his country from the global information infrastructure, but tech-savvy students and civic leaders established dial-up connections to Israel and Europe. As an example of a non-state actor response, Google provided a local Egyptian number that enabled people to tweet their comments on the uprisings and relay real-time accounts of the situation on the ground. Quite unintentionally, government agencies were severely affected by the shutdown, limiting their responses to the protests as well as causing significant financial losses. Middle class Egyptians, denied Internet access at home, also took to the streets in ever increasing numbers, some simply driven by the urge to find out what was going on. Meanwhile, the infosphere became the primary battleground. On one side, Egyptian security services started using Facebook and Twitter to anticipate movements of individual activists that led to a number of arrests. On the other, protestors used social media to create or bypass police barricades, whilst virtual leaders spread details of successful mobilization in the face of increasingly hapless attempts by the regime to stop them. Within a few weeks, there were widely circulating PDFs detailing how to pull off a successful protest. Social media had provided both an awareness of shared grievances, and widely disseminated strategies for action. The mobilizing slogan, “We Are All Khaled Said” helped ignite an uprising that ultimately led to the resignation of President Mubarak and the dissolution of the ruling National Democratic Party.

Libya

Prior to its revolution in 2011, the underlying societal problems in Libya mirrored many of those in Tunisia and Egypt. One of the key differences in the manner in which events unfolded in Libya, however, was the speed at which anti-government protest turned to violence, and then shifted to civil war requiring international intervention.

Following the fall of the Mubarak regime in Egypt, young Libyan Internet activists called for demonstrations on 17 February 2011, declaring it a "day of anger."[58] The response of the Libyan security forces included the highly unpopular arrest of an attorney who had been representing relatives of political prisoners massacred in a revolt a few years before. Mass demonstrations on the day of anger spread rapidly throughout the country. Those security forces that did not switch sides, countered the demonstrations with desperate brutality. *Al-Jamahiriya*, the Libyan state-owned television channel, responded by broadcasting non-stop patriotic songs, poetry recitations, and images of enthusiastic crowds showing support for the Libyan leader, Col. Mummar el-Qaddafi. *Al-Jamahiriya* even ran a written appeal: "for the dear brothers whose hobby is photography and video taping, please put up videos online that show the massive support for our beloved leader."[59] But even as this appeal was running, *Al Jazeera* was showing images of angry Libyan demonstrators throwing shoes at a giant screen carrying a live feed of Qaddafi's speech. As in Egypt, the infosphere became the primary battleground. A fierce information battle between regime supporters using state-run news media, and protestors who turned to social and foreign news media to seek the truth and win over hearts and

[58] BBC News, 'Libyan Security Official 'Sacked'', last modified 2011, accessed December 16, 2014, http://www.bbc.co.uk/news/world-africa-12490504.
[59]Nytimes.com, 'One Libyan Battle Is Fought In Social And News Media', last modified 2011, accessed December 16, 2014, http://www.nytimes.com/2011/02/24/world/middleeast/24iht-m24libya.html?_r=1&.

minds, occurred both inside and outside Libya. Social media not only provided the public with video footage of the regime's atrocities, it also created an international response as conditions moved towards civil war. The Arab League suspended Libya's membership and a United Nations resolution followed.

Islamic State

Having seized large swathes of land in Iraq and Syria, the rise of Islamic State (IS) in 2014 has been a dramatic example of group mobilization and modern insurgency. The organisation that grew out of the remnants of Al-Qaeda in Iraq, used the beginning of Ramadan 2014 to declare itself the first Caliphate since the Ottoman Empire, and its leader, Sheikh Abu Bakr Al-Baghdadi, the new Caliph for the global Ummah.[60] Part bandit, part criminal, part ideologue, part military, IS has created fear and outrage across the globe. What has been most striking about the success of IS is not necessarily its brutality, or even the speed at which it was able to seize territory, but the manner in which it has utilised sophisticated social media techniques to direct operations, terrorise elements of the population, recruit fighters, spread propaganda, and garner financial support. Its propaganda machine is so agile, slick and disciplined, that it has successfully projected a momentum and an unassailable image that far exceeds its real strength on the ground.

IS has developed a multidimensional, multilingual Info Ops campaign, spread across a variety of platforms, that has become increasingly sophisticated. It has an official media centre, Al-Hayat, which appears specifically to target the non-Arabic speaking,

[60]Abu Muhammad Al-'Adnani, 'This is the Promise of Allah', Al-Hayat Media, 2014; Abu Bakr Al-Baghdadi, 'A Message to the Mujahidin and the Muslim Ummah in the Month of Ramadan', Al-Hayat Media, 2014, http://www.gatestoneinstitute.org/documents/baghdadi-caliph.pdf , accessed 7 January 2015.

younger generation.[61] The quality of programming output is comparable to western mainstream broadcast standards. The production centre has its own logo, not dissimilar to that of Al-Jazeera, and produces a range of programmes from Twitter-friendly, minute-long "Mujatweets," to hour-long films, such as *Flames of War*, which even has its own Hollywood-style trailer.[62] Al-Hayat also publishes audio content, as well as an English-language magazine called Dabiq. Issue Two of the magazine had an article that likened the newly formed Caliphate to the Biblical Ark. The text was accompanied by images of the recently released Hollywood blockbuster *Noah*.[63] The magazine has also carried an interview with the Jordanian pilot, Muath al-Kaseasbeh, shortly after he was captured and before he was burned alive in a cage, allowing Al-Hayat to operate as its own news agency by disseminating information that news channels around the world would be forced to run.

In addition to material released from Al Hayat, IS also provides a steady stream of unofficial communications from its members. Through the use of simple messages, catchphrases, language targeted for different age groups, and striking imagery, all augmented by tactical actions on the battlefield, IS has proved particularly adept at shaping the perceptions, and polarising the support of its audiences. It has proved fluent in a wide variety of social media platforms including: YouTube; Twitter; WhatsApp; Kick; Diaspora; Wickr; Instagram and Tumblr. It has even produced Internet memes, such as #catsofjihad.[64] A particularly adept use of Twitter is the application "Fajr al-

[61] Steve Rose, 'The Isis Propaganda War: A Hi-Tech Media Jihad', *The Guardian*, last modified 2014, accessed January 8, 2015, http://www.theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war.
[62] Haroro J Ingram, 'Three Traits Of The Islamic State's Information Warfare', *The RUSI Journal* 159, no. 6 (2014): 4-11.
[63] Rose, *The Isis Propaganda War: A Hi-Tech Media Jihad*.
[64] Ibid.

Bashaer," or "Dawn of Good Tidings" (@Fajr991) which sends news and updates on IS fighting in Iraq and Syria, which can then be more widely distributed.[65] This effectively allows people who have not travelled to the region to join the online jihad from home. Those responsible for social media production have proved adept at tailoring the tweets so they appear on @Active Hashtags, an account that retweets the most trending hashtags of the day, thereby further amplifying their circulation.[66] IS has also proved highly effective at recruitment. One recruiting advert incorporating social media uses edited footage from the popular western video game *Grand Theft Auto*, and makes the claim that IS fighters can do for real on the battlefield what young men and women are doing in the virtual world when sat at home on their sofa.[67]

Figure 7. Different messages for different audiences

Hararo Ingram has analysed three traits of the IS information campaign: the use of a multidimensional, multi-platform approach that simultaneously targets friends and foes to enhance the reach, relevance, and resonance of its messaging; the synchronization of narrative and action to maximize operational and strategic effects in the field; and the

[65] Altahrir, news of Islam, Muslims, Arab Spring and special Palestine, 'How ISIS Conquered Social Media', last modified 2014, accessed January 7, 2015, https://altahrir.wordpress.com/2014/06/24/how-isis-conquered-social-media/.
[66] Ibid.
[67] Rose, *The Isis Propaganda War: A Hi-Tech Media Jihad*

centrality of the IS brand to its campaign.[68] His analysis of the three traits reveals a sophisticated systems approach that is ultimately tied to its politico-military actions on the battlefield. He concludes that it is the cumulative impact of all three traits that sets IS apart. The sophistication and emphasis given to this effort is significant. The infosphere is a virtual battlefield, playing to an audience that did not exist a generation ago. IS is tapping into the generation that has grown up immersed in social media and Internet content. It now dominates what is known, creates an aura of fear and mystery, and offers seductive attractions to a fantasy world of violence without restraint, under the guise of a religious crusade. IS encourages young girls like Aqsa Mahmood to leave Britain and join the jihadis in Syria. Blogging and tweeting under the name Umm Layth, she lionized the fighters she had met, bragged about the ease with which she had travelled and how satisfied she and her friends were with their new lives. She communicated directly on Twitter and Kick with people who wanted to know how they could join her. Given that Info Ops was recognised by both politicians and senior military commanders as one of the key strategic weaknesses of coalition operations in Afghanistan, there are clear lessons that can be learned from the group's actions.[69]

---

[68] Ingram, 'Three Traits Of The Islamic State's Information Warfare.

[69] See comments from J Scheffer in, 'Speech by NATO Secretary General, Jaap de Hoop Scheffer at the Seminar on Public Diplomacy in NATO- led Operations', 2007, http://www.nato.int/docu/speech/2007/s071008a.html, accessed 8 January 2015 and further comments in House of Commons Defence Committee: Operations in Afghanistan, Fourth Report of Session 2010-12 conclude that the UK Armed Forces have yet to incorporate fully strategic communications and "information and influence" operations into their campaigns, see http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/554/554.pdf accessed 8 January 2015.

Figure 8. Violence Without Restraint - Appeal and Intimidation

In Chapter Two, the impact of a country's relative dependence on information technology was discussed in the context of the higher vulnerability to web-based threats that it causes. Following the pattern of mass movements in Tunisia, Egypt, and Libya, virtual leaders have emerged to champion the IS cause. Hackers pledging allegiance to IS have brought the fight to the American mainland, as well as to the US military. In one of a number of cyber attacks in December 2014 and January 2015, hackers calling themselves *CyberCaliphate* took over the website and Twitter feed of American news station WBOC-TV in Salisbury, Maryland. They temporarily displayed the extremist group's black-and-white flag and a message saying, "I love you, ISIS." Hackers also took over *The Albuquerque Journal's* Twitter feed, replacing the newspaper's profile picture with an image that expressed support for Islamic militants. Numerous other posts followed, including warnings to residents that their confidential information was at risk.[70] These attacks were followed by an unprecedented wave of similar ones in France after the Charlie Hebdo offices were attacked by Islamic terrorists in Paris on 7 January 2015— France's head of cyber defence confirming that up to 19,000 websites had been

[70] English.alarabiya.net, last modified 2015, accessed January 8, 2015, http://english.alarabiya.net/en/media/digital/2015/01/08/Pro-ISIS-group-hijacks-U-S-station-s-site-paper-s-Twitter-feed.html.

hacked in the immediate aftermath.[71] And on 12 January 2015, in an embarrassing episode for the US military, hackers pledging allegiance to IS took control of US Central Command's Twitter and YouTube accounts, posting threatening messages and propaganda videos, along with some military documents.[72] Whilst it is not clear whether the hackers for all these episodes were members, or even genuine supporters of IS, the implication is that IS understands and is effectively applying methods of warfare in a new dimension. Unlike the western concept of media that has been related to the principle of Info Ops—sending messages as part of a military campaign—IS has demonstrated that it understands a virtual world exists in which tens of millions of people live and find their identities. IS currently operates in this virtual world with limited opposition.

Figure 9. US Central Command's Twitter Feed on 12 January 2015

In a somewhat clumsy effort to counter the IS militant propaganda, the U.S. State Department has launched its own Twitter account and established a presence on YouTube, Facebook and Tumblr using the title "Think Again Turn Away"

[71] Mashable, 'France: 19,000 Websites Hacked Since Charlie Hebdo Attack', last modified 2015, accessed February 4, 2015, http://mashable.com/2015/01/15/france-cyberattacks-charlie-hebdo/.
[72] Washington Post, 'U.S. Military Social Media Accounts Apparently Hacked By Islamic State Sympathizers', last modified 2015, accessed January 23, 2015, http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/.

(@ThinkAgain_DOS). It responds to themes in IS propaganda with counter messages to discredit their narrative, including links to articles about the harsh realities of life inside the so-called Caliphate. Whilst the State Department initiative is a step in the right direction, it currently lacks the sophistication and tone of appeal to young, savvy users. Besides being a government agency, therefore a source automatically discounted by its target audience, the State Department frequently comes across as a hectoring grown-up, thereby making its efforts less effective.

Similar moves are afoot within Europe where a strategy of counter-narratives and 'take-downs' seems to be emerging. In the UK, Police in the Counter Terrorism Internet Referral Unit are currently instigating the removal of 1,100 pieces of content a week—three quarters of them relating to Syria and IS.[73]

In December 2014, those trying to fight the information battle with IS had a victory with the arrest of virtual leader Mehdi Masroor Biswas in India, author of the highly influential pro-IS Twitter account @ShamiWitness. The ShamiWitness account had become a hub for propaganda and recruiting, with millions checking the Twitter feed every month. The arrest was significant for a couple of reasons. First, the account belonged to, and was operated by, an Indian business executive who tweeted from his office in Bangalore. Second, following the deactivation and suspension of numerous related IS Twitter accounts, it forced the organisation to change much of its modus

[73] BBC News, 'How The Battle Against IS Is Being Fought Online', last modified 2014, accessed January 8, 2015, http://www.bbc.com/news/magazine-29535343.

operandi online, as jihadis began to question the authenticity of other social media accounts and the extent to which they were being monitored by intelligence agencies.[74]

That said, it is not just intelligence agencies that IS and other global antagonists need to be concerned about. Eliot Higgins, the founder of Bellingcat and the Brown Moses blog, has shown what one man, using simple open source investigative analysis can do with social media and the Internet. In the process, he has demonstrated how, in a global information war, a nemesis can come from an unlikely source. In just three years, after what started as a hobby conducted from his home in Leicester, Higgins has established himself as one of the leading experts on the weaponry being deployed in Iraq and Syria. He has exposed the use of chemical weapons by the Assad regime, a hidden arms trail from Croatia to Syrian rebels, and undermined US claims not to be inflicting civilian casualties with Tomahawk missiles in Syria.[75] He has also, using self-taught geo-location techniques, been able to pinpoint the exact site of the murder by IS of American journalist James Foley, as well as embarrass Russia with detailed photographs allegedly tracking the movements through Ukraine of a Russian missile launcher linked to the downing of Malaysian airliner MH17 in July 2014.[76] Clearly, for military and foreign policy purposes, research of this kind must be accompanied by a clear understanding of the way that content is produced, who is sharing it, and whether it can be verified, but open source information, particularly that associated with social media, is increasingly

[74] Joyce Karam, *English.Alarabiya.Net*, last modified 2015, accessed February 9, 2015, http://english.alarabiya.net/en/perspective/features/2014/12/14/Shami-Witness-arrest-rattles-ISIS-cages-on-Twitter.html.
[75] Ian Burrell, 'With Isis, Assad And Putin Exposed, Who's Next On Citizen Journalist Eliot Higgins' List?', *The Independent*, last modified 2015, accessed February 5, 2015, http://www.independent.co.uk/news/people/profiles/with-isis-assad-and-putin-exposed-whos-next-on-citizen-journalist-eliot-higgins-list-9983831.html.
[76] Ibid.

able to provide a rich source of intelligence that can be used to reinforce decision-making and security policy. It is certainly an area that the military and intelligence agencies need to exploit better, and as a matter of urgency.

The examples presented here as case studies are a glimpse into a new era—and a new battleground controlled not by states and determined by any state policy, but a completely fluid and dynamic interplay of information. What is known is all that matters in this world—who knows what, and when, can lead to mass mobilization, as illustrated in Tunisia, Egypt, and Libya. In fact, war in the real world of Libya broke out as a result of the war first fought in the infosphere. IS has moved one step further, fighting a real and virtual war at the same time, crossing the boundaries between the two to present a powerful and attractive alternative to the western postmodern condition that a jaded, Muslim, immigrant generation immersed in social media and the Internet, finds hard to resist.

6. TEN RECOMMENDATIONS FOR A MORE DIGITALLY AGILE FORCE FIT FOR THE SOCIAL MEDIA ERA

If social networks are the hub of modern human interaction, and conflict is a chaotic, human activity that follows a cycle of adaptation and response, then the military needs to be optimised to exploit the opportunities and mitigate the threats that social networking using new media provides. The rising velocity of web-linked human interaction means that social media is going to play an increasingly important role in future conflict. The military need to operate effectively in this new battleground. To comprehend this environment, and its strategic and operational dimensions, two essential factors must be understood: the first is that people create virtual identities, some are fantasy, some are real; the second, is that people are empowered in the virtual world—popularity, influence, and self-actualization all come through social media. The first factor is significant because the authenticity of social media accounts is always open to question. Thus authenticity, or the belief that the source is authentic, is essential for operational success. Only with that belief will groups be mobilized, neutralized, or influenced. The second factor relates to the story of Eliot Higgins—the virtual world creates, as well as destroys, giants. Individuals have the power to become virtual leaders and in turn can destroy political leaders, or regimes. IS is arguably the first giant of the new battleground.

Operational planners and strategists must consider the hybrid nature of modern warfare. Unlike the currently accepted definition, this is a true hybrid of the virtual and the actual, coexisting in time, but not in space. Those who function effectively in both will succeed by gaining first the dominance over what is known in the virtual, and second, by displaying and employing effective measures in the actual. Listed below are

ten actions the military should take in order to optimise its capability for protecting the nation in the social media era:

1. **Alter the Mindset**. The current doctrinal view and attitude towards social media needs to change. It is much more than a tool for tweeting the latest MOD announcements, or a leisure time pursuit that poses a threat to operational security. Commanders at all levels need to understand the power and influence that social media can have on military operations. It is a dynamic tool that can simultaneously monitor, influence, and control society's behaviour. It is a vehicle to both understand and shape the operational environment.

2. **Select and Train Leaders for the Future Operating Environment**. Leaders are needed who are both comfortable with the multi-faceted nature of the cyber environment and who also think strategically. In addition to simply understanding and being able to navigate the cyber terrain, leaders will require a set of skills and attributes ranging from comprehending threats to evaluating and mitigating risk. They need to be comfortable operating with partners from across government, from non-governmental agencies and the private sector, and critically, be able to understand how complex systems work in the real world. Some of the traditional characteristics required for military leadership are evolving— commanders frequently need now not only to be able to lead in person, but also to build consensus and develop shared purpose via email, phone, or video teleconference, often with individuals or teams not under their direct military command. Finding such leaders will not happen by chance; they need to be selected, trained, and

developed. To quote James Carafano "a nation that wants to win online needs to build its arsenal of genius before the battle."[77]

3. **Revise and Update Extant Doctrine.** Extant doctrine needs to be updated to reflect the true impact and utility of social media within the operational environment. The current Information Operations and Media Operations publications are two specific examples that need substantial revision.

4. **Exploit the Shared Consciousness that Social Media Provides to Enhance Combat Effectiveness**. The principles underpinning social media, and the technology that various platforms use, has clear utility in the management of information flow within the military. The ability to provide the latest information (whether it be operational lessons identified, research development, or orders) instantaneously to a broad audience can enhance efficiency, break down elements of the 'need to know' culture that can hinder operational effectiveness, and can help realise the full potential and productivity of Service personnel. A conceptual shift from 'knowledge is power' to 'information sharing enables power' should be encouraged. Service personnel should be taught how to communicate better in the digital domain, mechanisms to share best practice should be improved, commanders should be empowered to take decisions, and innovation should be encouraged. Junior leaders should have ready access to knowledge transfer systems that enables them to read, share, and debate the latest enemy and friendly tactics, techniques, and procedures. Greater emphasis should be paid to the lateral

[77]Carafano, *Wiki At War*, 20.

transfer of knowledge rather than simply relying on the traditional top-down chain of command hierarchy. The speed, scrutiny, and sensitivity of the contemporary operating environment frequently means that the latter approach doesn't always provide sufficient focus on the critical information required by a subordinate commander to best achieve his or her mission. Online self-study programmes are a further area that should be capitalised on. Clearly a degree of financial investment is required and the appropriate security classification and protection would need to be in place, but this is an area that should not be squeezed out of the budget if a force fit for twenty-first century conflict is to be maintained.

5. **Better Integrate with Other Government Departments and Agencies**. Greater global connectivity and the transnational nature of certain threats requires closer collaboration between Government Departments and Agencies concerned with security. There is now no obvious boundary between oversees threats and risks to the UK homeland. Whilst the National Security Council works effectively at the strategic level, a more coherent whole-of-government approach to dealing with international and domestic security issues at the operational and tactical levels should be established. Clearer delineations of appropriate responsibility, accountability, and authority should be determined. Closer collaboration between military planners, GCHQ, the National Cyber Crime Unit, and the Research, Information and Communications Unit (RICU) for cyber and information operations, and the incorporation of best practice from the Metropolitan Police Internet Referral Unit, are two specific examples of where marked improvements could be readily achieved.

6. **Improve Cyber Awareness and Cyber Competence**. The security threats posed by the cyber domain are significant and growing. That said, an educated workforce and capable, competent leaders are the greatest competitive advantage the military can have for dealing with the challenges of rapidly changing technology. Competitive skills in the cyber domain should now be considered a core competence of the military. Offensive cyber operations are likely to be a routine element of future combat support, with military staff focused on attacking military platforms, battle procedure and networks as part of the orchestration of joint fires. Military activity will be synchronised with wider cyber effects. Training enhancements for military personnel should range from the general to the specialised. Annual cyber awareness training for all Service personnel, focused particularly on the threats from social media and the cyber domain, and similar to that conducted by the US Department of Defense, should be implemented. More specialised cyber and information operations training specific to role should also be developed and implemented.

7. **Better Utilise Social Media for Intelligence Purposes**. Eliot Higgins has demonstrated how social media can provide a rich source of information that can decisively contribute to the environmental intelligence picture and policymaking. The actions of IS have further shown how terrorists can exploit the Internet as a tool for recruiting, fund-raising, propaganda, and intelligence collection, as well as one to plan, coordinate, and control terrorist operations. Whether it is simple network analysis, source corroboration, or in the realm of special technical operations, the military needs to learn, adapt, exploit, and be one step ahead of

those who threaten the security of the UK. To effectively understand the new battleground, our intelligence capability needs to evolve from one that is effectively built around the fusion of largely secret intelligence, augmented loosely by open source, to a capability built around open source managed by Big Data analytics, and augmented by secret intelligence.

8. **Successfully Exploit Social Media in the Execution of Hybrid Warfare**. The study, planning, and successful execution of hybrid and unconventional warfare should deliberately incorporate and take account of the impact of social media on the public sphere. The ability to overcome obstacles of time and space by orchestrating multiple, near simultaneous, and sequential social movements has clear utility in this field. The concept of swarming, the use of social media to project power, as well as the multitude of other lessons identified from the Arab Spring, Islamic State and recent Russian activity should be incorporated into current doctrine, planning and practice.

9. **Build closer partnerships and leverage the expertise of the Private Sector**. The exponential growth of digital technology and its application, coupled with budgetary constraints, mean that individuals within the military cannot reasonably expect to always stay ahead of the curve in this domain. As a result, closer partnerships with the private sector are required to leverage the expertise, maximise the opportunities available, and build influence to best achieve military objectives. Such action ranges from greater collaboration with technology companies to help defeat security threats, to greater use of commercial intelligence, surveillance, and reconnaissance assets, to more general consultancy.

Companies such as *Social Flow* specialise in optimizing the delivery of messages on social networks. Their expertise, for example, could help improve the flow on information within the military at home, or be used to better target Info Ops when deployed.[78] In another example, organisations such as *C4ADS* specialise in investigative techniques and emerging analytical digital technologies to understand the drivers and enablers of global conflict, which has clear utility for future military operations.[79]

10. **Restructure Headquarters and Enhance the Career Profile for Cyber, Media and Information Operations**. If the centrality of influence, the criticality of information flow in enabling joint operations, and the importance of the cyber domain in the contemporary operating environment are subscribed to, then the current structure of conventional headquarters is not optimised to deliver successful military effect in this battlespace. Cyber, Info Ops and Media Ops should be at the heart of the headquarters structure and not just an adjunct to it, or worse still, absent. Furthermore, in the new battlespace, amongst the first consideration of commanders (and not just CIS staff) will be how to dominate the electromagnetic environment so the information, sensors, platforms, and weapons can be deployed, employed and synchronised in as uninhibited and protected manner as possible. The positioning and posting of suitable talent in these areas and career fields should be reinforced, with concomitant opportunities for promotion and progression.

[78] Social Flow's website can be accessed via the following link: http://www.socialflow.com.
[79] C4ADS's website can be accessed via the following link: http://www.c4ads.org.

7. CONCLUSION

In the past it has been relatively easy for Great Powers and governments to impose their values and manipulate the news. While still possible, it is now increasingly difficult because of advanced technology associated with the information revolution. The relationship between society, the government and military conduct has been decisively altered as a result of the evolution of social media. Although specific sites will come and go and Internet regulation will evolve, the phenomenon of social media and of global connectivity is here to stay. Indeed, its web is only going to spread wider and become increasingly dense. Social media is fast becoming the framework on which civil society is being built.

By using analysis of the evolution of social media and the propagation of the information revolution, by examining how the few can influence the many, and by identifying lessons from the Arab Spring and Islamic State's use of social media, this thesis has demonstrated how social media is changing global society and has already fundamentally altered the speed, scrutiny, and sensitivity of the military's operational environment. The Arab Spring has shown how a digitally connected crowd can serve as a mechanism for change and how social media can fan the flames of revolution once lit. Islamic State has shown how social media can serve as a means for recruiting, organising, sustaining, influencing, and terrorising different populations. Individuals such as Eliot Higgins have shown the intelligence value of successful analysis of social media, while the Power Law Distribution Curve demonstrates how the few can influence the many, and how social media can be used to increase the tempo of the OODA loop during military operations. British military doctrine, as it currently exists, does not sufficiently

address the impact of social media on the operational environment. And it certainly does not address the utility of social media in influencing social networks and crowd behaviour. It is a shortfall that particularly resonates in a strategic environment characterised by constant competition and one where information flow is so fundamental to the conduct of military operations. Ten recommendations are made to optimise the military's capability for protecting the nation in the social media era. They are as follows:

- Alter the Mindset
- Select and Train Leaders for the Future Operating Environment
- Revise and Update Extant Doctrine
- Exploit the Shared Consciousness that Social Media Provides to Enhance Combat Effectiveness
- Better Integrate with Other Government Departments and Agencies
- Improve Cyber Awareness and Cyber Competence
- Better Utilise Social Media for Intelligence Purposes
- Successfully Exploit Social Media in Unconventional Warfare Campaigns
- Build Closer Partnerships and Leverage the Experience of the Private Sector
- Restructure HQs and Enhance the Career Profile for Cyber, Media and Information Operations

The character of warfare is a dynamic organism that adapts to its environment and reflects how society operates. Studying, understanding, and conducting warfare in the twenty-first century means being able to engage in the economic, cultural, legal, social, and military dimensions of human competition. It means being able to wage war online. Social media is now a key part of that online world and it is of increasing importance because war, fundamentally, is a human endeavor and will therefore be influenced by social networks. That said, the current social media architecture should be considered to still be in its infancy. Equate it to the days of Alexander Graham Bell talking to his assistant across a rudimentary wire. As it spreads further, and only once society truly learns how to properly harness this new technology and these new ways of communicating will the full impact of social media be felt. As the organization with

primary responsibility for the UK's defence, along with interagency and private sector partners, the British military needs to be surfing the crest of the information wave, not desperately paddling to keep up. Commanders, at all levels, need to understand the hypersensitizing effect that social media has on the operational environment, as well as the importance of mobilising or neutralizing groups via social media to support a campaign or gain a strategic advantage. Failure to adapt will undermine the effectiveness of military action and the nation's confidence in it as an instrument of national power.

BIBLIOGRAPHY

Abu Bakr Al-Baghdadi. “A Message to the Mujahidin and the Muslim Ummah in the Month of Ramadan.”Al-Hayat Media, 2014. Accessed January 7 2015. http://www.gatestoneinstitute.org/documents/baghdadi-caliph.pdf.

Altahrir. “How ISIS Conquered Social Media”. Last modified 2014. Accessed January 7, 2015. https://altahrir.wordpress.com/2014/06/24/how-isis-conquered-social-media/.

BBC News. “How The Battle Against IS Is Being Fought Online.” Last modified 2014. Accessed January 8, 2015. http://www.bbc.com/news/magazine-29535343.

BBC News. “Libyan Security Official 'Sacked.” Last modified 2011. Accessed December 16, 2014. http://www.bbc.co.uk/news/world-africa-12490504.

BBC News. “Zuckerberg's Letter To Investors.” Last modified 2012. Accessed December 10, 2014. http://www.bbc.com/news/technology-16859527.

Beaumont, Peter. “The Truth About Twitter, Facebook And The Uprisings In The Arab World.” *The Guardian*. Last modified 2011. Accessed January 28, 2015. http://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings-arab-libya.

Biddle, Tami Davis. *Rhetoric And Reality In Air Warfare*. Princeton, N.J.: Princeton University Press, 2002.

Blank, Stephen. “Russian Information Warfare As Domestic Counterinsurgency”. *American Foreign Policy Interests* 35, no. 1 (2013): 31-44.

Boyd, Danah M., and Nicole B. Ellison. “Social Network Sites: Definition, History, And Scholarship.” *Journal of Computer-Mediated Communication* 13, no. 1 (2007): 210-230.

Brunner, Elgin M, and Myriam Dunn Cavelty. “The Formation Of Information By The US Military: Articulation And Enactment Of Infomanic Threat Imaginaries On The Immaterial Battlefield Of Perception.” *Cambridge Review of International Affairs* 22, no. 4 (2009): 629-646.

Burrell, Ian. “With Isis, Assad And Putin Exposed, Who's Next On Citizen Journalist Eliot Higgins' List?” *The Independent*. Last modified 2015. Accessed February 5, 2015. http://www.independent.co.uk/news/people/profiles/with-isis-assad-and-putin-exposed-whos-next-on-citizen-journalist-eliot-higgins-list-9983831.html.

Carafano, James Jay. *Wiki At War*. College Station: Texas A&M University Press, 2012.

Castells, M. “The New Public Sphere: Global Civil Society, Communication Networks, And Global Governance.” *The Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 78-93.

Cavazza, Frederic. 'Social Media Landscape 2014 - Fredcavazza.Net'. *Fredcavazza.Net*.

Last modified 2014. Accessed January 3, 2015. http://www.fredcavazza.net/2014/05/22/social-media-landscape-2014/.

CIA.gov,. “The World Factbook.” Last modified 2015. Accessed January 4, 2015. https://www.cia.gov/library/publications/the-world-factbook/.

Clarke, Richard A, and Robert K Knake. *Cyber War*. New York: Ecco, 2010.

Cochrane, Feargal. *Ending Wars*. Cambridge: Polity, 2008.

English.alarabiya.net,. Last modified 2015. Accessed January 8, 2015. http://english.alarabiya.net/en/media/digital/2015/01/08/Pro-ISIS-group-hijacks-U-S-station-s-site-paper-s-Twitter-feed.html.

Fuchs, C. “Social Media, Riots, And Revolutions.” *Capital & Class* 36, no. 3 (2012): 383-391.

Galeotti, Mark. “The Gerasimov Doctrine' And Russian Non-Linear War.” *In Moscow's Shadows*. Last modified 2014. Accessed October 29, 2014. http://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Ghonim, Wael. *Revolution 2.0*. Boston: Houghton Mifflin Harcourt, 2012.

Gov.uk,. 'Cyber Primer - Publications - GOV.UK'. Last modified 2014. Accessed February 23, 2015. https://www.gov.uk/government/publications/cyber-primer.

Hannigan, Robert. “The Web Is A Terrorists Command and Control Network Of Choice - FT.Com.” *Financial Times*. Last modified 2014. Accessed January 4, 2015. http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3LFmC9nwL.

Haythornthwaite, Caroline. “Social Networks And Internet Connectivity Effects.” *Information, Communication & Society* 8, no. 2 (2005): 125-147.

Hochwald, Thorsten. 'How Do Social Media Affect Intra-State Conflicts Other Than War?'. *ConnQJ* 12, no. 3 (2013): 9-37.

Howard, Philip N., and Muzammil M. Hussain. “The Role Of Digital Media.” *Journal of Democracy* 22, no. 3 (2011): 35-48.

Ingram, Haroro J. “Three Traits Of The Islamic State’s Information Warfare.” *The RUSI Journal* 159, no. 6 (2014): 4-11.

Insight.globalwebindex.net,. “GWI Social - Q2 2014 Globalwebindex Report Series.” Last modified 2014. Accessed December 9, 2014. http://insight.globalwebindex.net/gwi-social-q2-2014.

Investor.fb.com,. “Facebook Reports Third Quarter 2014 Results – Facebook.” Last modified 2014. Accessed January 5, 2015. http://investor.fb.com/releasedetail.cfm?ReleaseID=878726.

Kaku, Michio. *Physics Of The Future*. New York: Doubleday, 2011.

Kaplan, Andreas M., and Michael Haenlein. "Users Of The World, Unite! The Challenges And Opportunities Of Social Media." *Business Horizons* 53, no. 1 (2010): 59-68.

Karam, Joyce. *English.Alarabiya.Net*. Last modified 2015. Accessed February 9, 2015. http://english.alarabiya.net/en/perspective/features/2014/12/14/Shami-Witness-arrest-rattles-ISIS-cages-on-Twitter.html.

Khondker, Habibul Haque. "Role Of The New Media In The Arab Spring." *Globalizations* 8, no. 5 (2011): 675-679.

Lawson, Sean. "The US Military's Social Media Civil War: Technology As Antagonism In Discourses Of Information-Age Conflict." *Cambridge Review of International Affairs* 27, no. 2 (2013): 226-245.

Levy, Steven. "Mark Zuckerberg On Facebook Home, Money, And The Future Of Communication." *Wired*. Last modified 2013. Accessed January 4, 2015. http://www.wired.com/2013/04/facebookqa/.

Lonsdale, David J. *The Nature Of War In The Information Age*. London: Frank Cass, 2004.

Mackinley, John. "The Next Security Era For Britain." *Prism* 3, no. 2 (2014): 51-60.

Madway, Gabriel. "Twitter Remakes Website, Adds New Features." *Reuters*. Last modified 2014. Accessed January 3, 2015. http://www.reuters.com/article/2010/09/15/us-twitter-website-idUSTRE68E02620100915.

Mashable. "France: 19,000 Websites Hacked Since Charlie Hebdo Attack." Last modified 2015. Accessed February 4, 2015. http://mashable.com/2015/01/15/france-cyberattacks-charlie-hebdo/.

McLuhan, Marshall and Quentin Fiore, *The Medium is the Massage*. New York: Random House, 1967.

Ministry of Defence. *Cyber Operations - The Defence Contribution.* London: MOD, 2013.

Ministry of Defence. *Cyber Primer*. London: MOD, 2013.

Ministry of Defence. *Future Character Of Conflict*. London: MOD, 2010.

Nytimes.com. "One Libyan Battle Is Fought In Social And News Media." Last modified 2011. Accessed December 16, 2014. http://www.nytimes.com/2011/02/24/world/middleeast/24iht-m24libya.html?_r=1&.

President Obama, Barack. "Remarks By The President At The United States Military Academy Commencement Ceremony." *The White House*. Last modified 2014.

Accessed November 17, 2014. http://www.whitehouse.gov/the-press-office/2014/05/28/remarks-president-united-states-military-academy-commencement-ceremony.

Phares, Walid. *The War Of Ideas*. New York: Palgrave Macmillan, 2007.

Rose, Chris. "The Security Implications Of Ubiquitous Social Media." *International Journal of Management and Information Systems* 15, no. 1 (2011): 35-39.

Rose, Steve. "The Isis Propaganda War: A Hi-Tech Media Jihad." *The Guardian*. Last modified 2014. Accessed January 8, 2015. http://www.theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war.

Schaller, R.R. 'Moore's Law: Past, Present And Future'. *IEEE Spectr.* 34, no. 6 (1997): 52-59.

Shirky, Clay. *Here Comes Everybody*. New York: Penguin Press, 2008.

Surowiecki, James. *The Wisdom Of Crowds*. New York: Doubleday, 2004.

Thompson, Robin. "Radicalization And The Use Of Social Media." *Journal of Strategic Security* 4, no. 4 (2011): 167-190.

Timpane, John. "The Social Media Side Of War." *Philadelphia Inquirer* (2014): 1-3.

Toffler, Alvin, and Heidi Toffler. *War And Anti-War*. Boston: Little, Brown, 1993.

VARGAS, JOSE. "How An Egyptian Revolution Began On Facebook." *Nytimes.Com*. Last modified 2012. Accessed November 19, 2014. http://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html?pagewanted=all&_r=1&.

Vitale, Heather Marie, and James Keagle. "A Time To Tweet, As Well As A Time To Kill: ISIS's Projection Of Power In Iraq And Syria." *Defense Horizons* 77 (2014): 1-12.

Washington Post,. "U.S. Military Social Media Accounts Apparently Hacked By Islamic State Sympathizers." Last modified 2015. Accessed January 23, 2015. http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/.

We Are Social,. "Blog." Last modified 2014. Accessed January 4, 2015. http://wearesocial.com.

Wikipedia,. "Long Tail." Last modified 2015. Accessed January 4, 2014. http://en.wikipedia.org/wiki/Long_tail#mediaviewer/File:Long_tail.svg.

VITA

After graduating from Edinburgh University, Andrew Ridland commissioned into The Royal Green Jackets in 2000 and spent his early career as an Armoured Infantry Platoon Commander, Company Operations Officer and Intelligence Officer seeing active service in Bosnia, Northern Ireland and Iraq. Away from the Battalion he served as ADC to GOC 5 Div and as SO3 G3 (Ops/Cts) in the Army Headquarters. He was the Operations Officer of 2 Rifles in 2006-2007, which included a second deployment to Iraq on Op Telic 9 as part of the Basra City Battlegroup.

Following completion of the Intermediate Command and Staff Course (Land) in 2009, he spent two years in the Ministry of Defence working in Army Resources and Plans, during which time he was heavily involved in the Strategic Defence and Security Review. Following this, he commanded A Company 3 Rifles, which included a deployment to Afghanistan on Op Herrick 16 where the Company was in a ground-holding role in Nahr-e-Saraj. He was then Chief of Staff 20th Armoured Brigade, before being promoted to Lieutenant Colonel and selected to attend the Joint Forces Staff College in Norfolk, USA.